Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A secure passcode authentication system, the system comprising:

an Access Control Server (ACS) configured to receive a request for passcode authentication of a Primary Account Number (PAN) from a merchant server, and configured to request a passcode corresponding to the PAN from a cardholder device, wherein the ACS is associated with an issuer of the PAN;

a front end Hardware Security Module (HSM) coupled to the ACS, and configured to receive the passcode in an encrypted format and generate an encrypted passcode using a local encryption key; and

a back end HSM configured to receive the encrypted passcode from the front end HSM and further configured to recover a clear form of the passcode, generate a back end encrypted passcode, and communicate the back end encrypted passcode to an authentication network, wherein the system authenticates the passcode, wherein the ACS is further configured to receive an authentication message from the authentication network.

2. (Original) The system of Claim 1, wherein the request for passcode authentication comprises a request for a Personal Identification Number (PIN) authentication.

3. (Canceled)

4. (Original) The system of Claim 1, wherein the ACS is further configured to generate a unique transaction identification and include the unique transaction identification as a hidden field in the request for the passcode.

5. (Original) The system of Claim 4, wherein the front end HSM is configured to generate a hash value based in part on the unique transaction identification, and wherein the ACS is configured to include the hash value as an additional hidden field in the request for the passcode.

6. (Original) The system of Claim 1, wherein the request for the passcode includes an instruction to direct the passcode to the front end HSM.

7. (Original) The system of Claim 1, wherein the front end HSM comprises a software HSM.

8. (Original) The system of Claim 1, wherein the front end HSM comprises a hardware HSM.

9. (Canceled)

10. (Previously Presented) The system of Claim 1, wherein the encrypted format comprises a Secure Sockets Layer (SSL) encrypted format.

11. (Original) The system of Claim 1, wherein the front end HSM is configured to receive a cardholder encrypted passcode from the ACS.

12. (Original) The system of Claim 1, wherein the front end HSM is configured to receive a cardholder encrypted passcode from a cardholder device.

13. (Original) The system of Claim 1, wherein the back end HSM is configured to generate the back end encrypted passcode by generating a PINBLOCK using the clear form of the passcode and encrypting the PINBLOCK using an Acquirer Working Key (AWK).

14. (Original) The system of Claim 1, wherein the authentication network comprises an Internet Payment Gateway Server (IPGS).

15. (Original) The system of Claim 14, wherein the authentication network further comprises an issuer server coupled to the IPGS.

16. (Original) A secure passcode authentication system, the system comprising:

an Access Control Server (ACS) configured to receive a request for Personal Identification Number (PIN) authentication of a Primary Account Number (PAN), and configured to generate a request for a PIN corresponding to the PAN, the request for the PIN including hidden fields comprising a unique transaction identifier and a hash value;

a front end Hardware Security Module (HSM) coupled to the ACS, and configured to generate the hash value based in part on the unique transaction identifier, and further configured to receive an encrypted PIN, decrypt the PIN to recover a clear form of the PIN, and generate a local encrypted PIN using a local encryption key; and

a back end HSM configured to receive the local encrypted PIN from the front end HSM and further configured to recover a clear form of the PIN from the local encrypted PIN, generate an Acquirer Working Key (AWK) encrypted PIN, and communicate the AWK encrypted PIN to an authentication network.

17. (Original) The system of Claim 16, wherein the front end HSM generates the local encrypted key using a triple DES algorithm.

18. (Original) A secure passcode authentication system, the system comprising:

an Access Control Server (ACS) configured to receive a request for Personal Identification Number (PIN) authentication of a Primary Account Number (PAN), and configured to generate a request for a PIN corresponding to the PAN, the request for the PIN including an instruction to provide the PIN to a destination address; and

a front end Hardware Security Module (HSM) having said destination address and coupled to the ACS, and configured to receive an encrypted PIN, decrypt the PIN to recover a clear form of the PIN, and generate an Acquirer Working Key (AWK) encrypted PIN using an

AWK encryption key, and configured to communicate the AWK encrypted PIN to an authentication network.

19. (Previously Presented) A method for providing secure passcode authentication, the method comprising:

requesting a Personal Identification Number (PIN) corresponding to a Primary Account Number (PAN) wherein requesting the PIN includes generating a unique transaction identifier, generating a hash value with a front end Hardware Security Module (HSM) based in part on the unique transaction identifier, generating a query having the unique transaction identifier and hash value as fields in the query, and communicating the query;

receiving an encrypted PIN in the front end Hardware Security Module (HSM) in response to the request;

generating a PINBLOCK based in part on the encrypted PIN;

encrypting the PINBLOCK using a local key in a front end Hardware Security Module (HSM) to generate a local key encrypted PINBLOCK;

decrypting the local key encrypted PINBLOCK with a back end HSM;

generating a back end encrypted PIN with the back end HSM;

communicating the back end encrypted PIN to an authentication network; and

receiving an authentication response from the authentication network.

20. (Canceled)

21. (Original) The method of Claim 19, wherein requesting the PIN comprises:

generating a query having an instruction directing a query response be directed to a destination address corresponding to the front end HSM; and

communicating the query over an Internet connection to a cardholder device.

22. (Original) The method of Claim 19, wherein receiving the PIN comprises receiving a Secure Sockets Layer (SSL) encrypted PIN.

23. (Original) The method of Claim 22, wherein receiving the PIN further comprises receiving the SSL encrypted PIN at an Access Control Server (ACS).

24. (Original) The method of Claim 22, wherein receiving the PIN further comprises receiving the SSL encrypted PIN from a cardholder device at the front end HSM.

25. (Original) The method of Claim 19, wherein the front end HSM comprises a software HSM implementation within an Access Control Server (ACS).

26. (Original) The method of Claim 19, wherein encrypting the PINBLOCK comprises encrypting the PINBLOCK using a triple DES encryption algorithm.

27. (Original) The method of Claim 19, wherein generating the back end encrypted PIN comprises:

generating a back end PINBLOCK from a clear form of the PIN; and

encrypting the PIN with the back end HSM using an Acquirer Working Key (AWK).

28. (Previously Presented) A method for providing secure passcode authentication, the method comprising:

receiving an encrypted Personal Identification Number (PIN) corresponding to a Primary Account Number (PAN) in a front end Hardware Security Module (HSM) over a Secured Sockets Layer (SSL) internet connection between a cardholder device and the front end HSM, wherein the PIN is exclusively SSL encrypted;

decrypting the encrypted PIN in the front end Hardware Security Module (HSM) to generate a clear form of the PIN;

generating a PINBLOCK based in part on the clear form of the PIN;

generating in a back end HSM a back end encrypted PIN based in part on the PINBLOCK;

communicating the back end encrypted PIN to an authentication network; and

receiving an authentication response from the authentication network.

29. (Original) The method of Claim 28, wherein the front end HSM comprises the back end HSM.

30. (Canceled)

31. (Original) The method of Claim 28, wherein generating the back end encrypted PIN comprises generating an Acquirer Working Key (AWK) encrypted PIN.

32. (Previously Presented) A method for providing secure passcode authentication, the method comprising:

generating encryption data;

querying a cardholder for a Personal Identification Number (PIN) corresponding to a Primary Account Number (PAN);

receiving in a front end Hardware Security Module (HSM) an encrypted PIN and at least a portion of the encryption data from the cardholder in response to the query;

generating a clear form of the PIN based in part on the encrypted PIN;

generating a PINBLOCK based in part on the clear form of the PIN;

encrypting the PINBLOCK in a front end Hardware Security Module (HSM) using triple DES encryption to generate an encrypted PIN (EPIN);

decrypting the EPIN in a back end HSM to recover the clear form of the PIN;

encrypting the clear form of the PIN in the back end HSM using an Acquirer Working Key (AWK) to generate an AWK encrypted PIN;

communicating the AWK encrypted PIN to an authentication network; and

receiving an authentication response.

33. (Previously Presented) The system of Claim 1, further comprising a Directory Server configured to verify a Primary Account Number's eligibility to participate in secure passcode authentication.

34. (Previously Presented) The system of Claim 18, wherein the instruction to provide a PIN to a destination address is an HTTP redirect instruction.

35. (Previously Presented) The method of claim 32, wherein the encryption data comprises a transaction ID, a base redirection url, an http redirect type.

36. (Currently Amended) A method for providing secure passcode authentication, the method comprising:

generating encryption data, wherein the encryption data comprises a transaction ID, a base redirection url, and an http redirect type, ~~The method of claim 35~~ wherein the encryption data further comprises a hashed message authentication code based on the transaction ID, the base redirection URL, and the http redirect type [[.]];

querying a cardholder for a Personal Identification Number (PIN) corresponding to a Primary Account Number (PAN);

receiving in a front end Hardware Security Module (HSM) an encrypted PIN and at least a portion of the encryption data from the cardholder in response to the query;

generating a clear form of the PIN based in part on the encrypted PIN;

generating a PINBLOCK based in part on the clear form of the PIN;

encrypting the PINBLOCK in a front end Hardware Security Module (HSM) using triple DES encryption to generate an encrypted PIN (EPIN);

decrypting the EPIN in a back end HSM to recover the clear form of the PIN;

encrypting the clear form of the PIN in the back end HSM using an Acquirer Working Key (AWK) to generate an AWK encrypted PIN;

communicating the AWK encrypted PIN to an authentication network; and

receiving an authentication response.

37. (New) The method of claim 1 wherein the access control server, the front end hardware security module, and the back end are co-located.

38. (New) The system of Claim 1, wherein the ACS is further configured to return an authentication response to the merchant server.